UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/670,129	09/26/2000	Vladimir R. Pisarsky	US000262	5658

7590   04/26/2004

Michael E Marion
Corporate Patent Counsel
U S Philips Corporation
580 White Plains Road
Tarrytown, NY 10591

EXAMINER
SHARON, AYAL I

ART UNIT	PAPER NUMBER
2123	

DATE MAILED: 04/26/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.		Applicant(s)	
Office Action Summary	09/670,129		PISARSKY, VLADIMIR R.	
	Examiner		Art Unit	
	Ayal I Sharon		2123	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>2/6/04</u>.

2a)☒ This action is **FINAL.**   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,5,6 and 10-16* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,5,6 and 10-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

Introduction

1. Claims 1-9 of U.S. Application 09/670,129 filed on 09/26/2000 are presented for

examination. In paper #5, filed on 2/6/04, claims 1-2 and 5-6 were amended,

claims 3-4 and 7-9 were cancelled, and claims 10-16 were added.

Claim Rejections - 35 USC § 101

2. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of
> matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the
> conditions and requirements of this title.

3. **Claim 1-2, 5-6, and 10-16 are rejected under 35 U.S.C. 101 because the**

claimed invention the claimed invention is directed to non-statutory subject

matter.

4. The output of the invention claimed in Claims 1 and 5 is "a value of a quantity

according to a respective mathematical function." This abstract result, "a value of

a quantity", is not concrete, useful, or tangible. Dependent Claims 2 and 6 inherit

this defect.

5. In addition, there is no output cited for the method claimed in Claim 10. There is

merely the claimed final step of "determining whether there is a mismatch

between the received numerical values and the simulated numerical values."

Therefore, the result of the determination is not concrete, useful, or tangible.

Dependent Claims 11-16 inherit this defect.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

   The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. **Claims 1-2 and 5-6 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.**

8. Independent Claims 1 and 5 are vague as to what constitutes "evaluating a result supplied by the primary system with respect to an outcome calculated by the simulator in order to monitor the primary system."

   More importantly, Claims 1 and 5 are vague in regards to what is done with the evaluated result.

   Claims 1 and 5 also claim "Calculat[ing] ... a value of a quantity according to a respective mathematical function." The claims are vague as to what the value represents, and what constitutes the mathematical function.

   Claims 1 and 5 also refer to "primary" and "secondary" tasks, yet the claims are vague as to what these tasks are.

   Dependent Claims 2 and 6 inherit this defect.

9. **Claims 10-16 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.**

10. Independent Claim 10 is vague as to what constitutes "determining whether there is a mismatch between the received numerical values and the simulated numerical values."

     More importantly, Claim 10 is vague in regards to what is done with the determination. There is no output cited for the invention claimed in Claim 10, merely a final step of "determining whether there is a mismatch between the received numerical values and the simulated numerical values."

     Claim 10 also refers to "primary" and "secondary" tasks, yet the claim is vague as to what these tasks are.

     Dependent Claims 11-16 inherit this defect.

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. The prior art used for these rejections is as follows:

13. Hershey et al., U.S. Patent 5,414,833. (Henceforth referred to as "**Hershey**").

14. Ilgun, K. et al. "State Transition Analysis: A Rule-Based Intrusion Detection

Approach." IEEE Transaction on Software Engineering. March 1995. Vol.21,

Issue 3, pp.181-199. (Henceforth referred to as "**Ilgun**").

15. Sekar, R. et al. "Synthesizing Fast Intrusion Prevention / Detection Systems from

High-Level Specifications." Proc. of the 8th USENIX Security Symposium. August

23-26, 1999. (Henceforth referred to as "**Sekar**").

16. The claim rejections are hereby summarized for Applicant's convenience. The

detailed rejections follow.

17. **Claims 1 and 5 are rejected under 35 U.S.C. 103(a) as being unpatentable**

over Hershey in view of Ilgun.

18. **Claims 2 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable**

over Hershey in view of Ilgun and further in view of Sekar.

19. In regards to Claim 1, Hershey teaches the following limitations:

> 1. (Currently Amended) A monitoring system comprising:
>   a primary system with multiple devices; and
> Examiner interprets the "primary system with multiple devices" as being a
> network. Hershey teaches the use of security agents and a network security
> manager. (See Hershey: col.7, lines 22-50; col.6, lines 46-65; Fig.24; col.11, line
> 35 to col.12, line 25)
>
>   wherein each respective one of the devices comprises a respective
> finite state machine;
> (See Hershey: Abstract; and col.11, line 35 to col.12, line 25;)
>
> each respective state machine calculates, per time step, a value of a quantity according to a
> respective mathematical function; and
> (See Hershey: col.9, line 65 to col.10, line 7, which teaches that "The first FSM is
> called the predecessor FSM, and it is configured to detect the first component
> pattern. The second FSM is called the successor FSM, and it is configured to
> detect the second component pattern. The first FSM will send a starting signal to
> the second FSM, when the first FSM has successfully detected the first

component pattern." Examiner interprets the "detection" as being a Boolean mathematical function equivalent to "if x=y then ..., else ...")

wherein each respective device has a respective computational resource;
(See Hershey: col.10, lines 46-48, which teach that "Each FSM consists of an address register and a memory")

each respective one of the devices performs a respective primary task using the respective resource;
(See Hershey: col.9, lines 62-67, which teach that "The adaptive, active monitor comprises two finite state machines (FSM) which are constructed to detect the occurrence of a characteristic data pattern having two consecutive component bit patterns.")

depending on usage of the resource for the respective primary task, each respective device performs a respective secondary task for reducing availability of the respective computational resource;
(See Hershey: col.10, lines 60-65, which teach that "Each memory has a plurality of data storage locations, each having a first portion with n-X bits, to be output to the address register as part of the next address. Many of the memory locations have a second portion which stores a command to reset the address register if the FSM fails to detect its designated component bit pattern.")

and the respective secondary task comprises calculating the quantity using adapting a length of the respective history.
(See Hershey: col.10, lines 60-65, which teach that "Each memory has a plurality of data storage locations, each having a first portion with n-X bits, to be output to the address register as part of the next address. Many of the memory locations have a second portion which stores a command to reset the address register if the FSM fails to detect its designated component bit pattern.")

However, Hershey does not expressly teach the following limitations:

a simulator for simulating behavior of the primary system;
wherein:

the monitoring system evaluates a result supplied by the primary system with respect to an outcome calculated by the simulator in order to monitor the primary system

Hershey's teaches a security agent where "The security agent includes an

adaptive, active monitor using finite state machines that can be dynamically

programmed in the event it becomes necessary to dynamically reconfigure it to

provide real time detection of the presence of a suspected offending virus". (See Hershey: Abstract).

Hershey also teaches that "Each FSM consists of an address register and a memory" (See Hershey: col.10, lines 46-48) and "Many of the memory locations have a second portion which stores a command to reset the address register if the FSM fails to detect its designated component bit pattern." (See Hershey: col.10, lines 60-65).

However, Hershey does not expressly teach how the "designated component bit pattern" is designated, nor, more specifically, that the "designated component bit pattern" is calculated by a simulator.

Ilgun, on the other hand, teaches the use of a model-based intrusion detection method, "The objective is to build *scenario models* that represent the characteristic behavior of intrusions. This allows administrators to generate their representation of the penetration abstractly, which shifts the burden of determining what audit records are part of a suspect sequence to the expert system." (See Ilgun: p.183, Section D).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Hershey with those of Ilgun, by using a simulator to generate the "designated component bit pattern", because doing so would enable the user to "model intrusions at a higher level of transactions than audit records." (See Ilgun: p.183, Section D).

20. In regards to Claim 2, Hershey teaches the following limitations:

2. (Currently Amended) The system of claim 1, wherein:
the respective mathematical function has as arguments:

the value of the quantity calculated at a preceding time step by at least another one of the state machines;
(See Hershey: col.9, line 65 to col.10, line 7, which teaches that "The first FSM is called the predecessor FSM, and it is configured to detect the first component pattern. The second FSM is called the successor FSM, and it is configured to detect the second component pattern. The first FSM will send a starting signal to the second FSM, when the first FSM has successfully detected the first component pattern.")

a respective history of values assumed by the quantity calculated by the respective state machine;
(See Hershey: col.10, lines 60-65, which teach that "Each memory has a plurality of data storage locations, each having a first portion with n-X bits, to be output to the address register as part of the next address. Many of the memory locations have a second portion which stores a command to reset the address register if the FSM fails to detect its designated component bit pattern.")

a respective control code determined by content present in a memory of the respective device at the time step;
(See Hershey: col.10, lines 60-65, which teach that "Each memory has a plurality of data storage locations, each having a first portion with n-X bits, to be output to the address register as part of the next address. Many of the memory locations have a second portion which stores a command to reset the address register if the FSM fails to detect its designated component bit pattern.")

However, Hershey does not expressly teach the following limitation:

the respective mathematical function is such that the quantity assumes a stochastic behavior.

Sekar, on the other hand, does teach this. Sekar teaches (Section 4 "Runtime Model", paragraph 2; also Fig.3) that "An EFSA [extended finite-state automata] is normally non-deterministic. ... A deterministic EFSA (DEFA for short) is an EFSA in which at most one of the transitions is enabled in any state of the EFSA."

It would have been obvious to one of ordinary skill in the art at the time the

invention was made to modify the teachings of Hershey with those of Sekar,

because Sekar teaches about the inherent properties of finite-state automata.

21. In regards to Claim 5, Hershey teaches the following limitations:

5. (Currently Amended) A method of enabling protection of a primary system that has multiple devices, the method comprising:
Examiner interprets the "primary system with multiple devices" as being a network. Hershey teaches the use of security agents and a network security manager. (See Hershey: col.7, lines 22-50; col.6, lines 46-65; Fig.24; col.11, line 35 to col.12, line 25)

wherein each respective one of the devices comprises a respective finite state machine;
(See Hershey: Abstract; and col.11, line 35 to col.12, line 25;)

the respective state machine calculates per time step a value of a quantity according to a respective mathematical function;
(See Hershey: col.9, line 65 to col.10, line 7, which teaches that "The first FSM is called the predecessor FSM, and it is configured to detect the first component pattern. The second FSM is called the successor FSM, and it is configured to detect the second component pattern. The first FSM will send a starting signal to the second FSM, when the first FSM has successfully detected the first component pattern." Examiner interprets the "detection" as being a Boolean mathematical function equivalent to "if x=y then ..., else ...")

each respective device has a respective computational resource;
(See Hershey: col.10, lines 46-48, which teach that "Each FSM consists of an address register and a memory")

each respective one of the devices performs a respective primary task using the respective resource;
(See Hershey: col.9, lines 62-67, which teach that "The adaptive, active monitor comprises two finite state machines (FSM) which are constructed to detect the occurrence of a characteristic data pattern having two consecutive component bit patterns.")

the method comprises enabling each respective device to perform a respective secondary task, depending on the respective primary task, for reducing availability of the respective computational resource; and
(See Hershey: col.10, lines 60-65, which teach that "Each memory has a plurality of data storage locations, each having a first portion with n-X bits, to be output to the address register as part of the next address. Many of the memory locations

have a second portion which stores a command to reset the address register if the FSM fails to detect its designated component bit pattern.")

the respective secondary task; comprises calculating the quantity using adapting a length of the respective history.
(See Hershey: col.10, lines 60-65, which teach that "Each memory has a plurality of data storage locations, each having a first portion with n-X bits, to be output to the address register as part of the next address. Many of the memory locations have a second portion which stores a command to reset the address register if the FSM fails to detect its designated component bit pattern.")

However, Hershey does not expressly teach the following limitations:

simulating a behavior of the primary system; and

evaluating a result supplied by the primary system with respect to an outcome calculated by the simulators

Hershey's teaches a security agent where "The security agent includes an adaptive, active monitor using finite state machines that can be dynamically programmed in the event it becomes necessary to dynamically reconfigure it to provide real time detection of the presence of a suspected offending virus". (See Hershey: Abstract).

Hershey also teaches that "Each FSM consists of an address register and a memory" (See Hershey: col.10, lines 46-48) and "Many of the memory locations have a second portion which stores a command to reset the address register if the FSM fails to detect its designated component bit pattern." (See Hershey: col.10, lines 60-65).

However, Hershey does not expressly teach how the "designated component bit pattern" is designated, nor, more specifically, that the "designated component bit pattern" is calculated by a simulator.

Ilgun, on the other hand, teaches the use of a model-based intrusion

detection method, "The objective is to build *scenario models* that represent the

characteristic behavior of intrusions. This allows administrators to generate their

representation of the penetration abstractly, which shifts the burden of

determining what audit records are part of a suspect sequence to the expert

system." (See Ilgun: p.183, Section D).

It would have been obvious to one of ordinary skill in the art at the time the

invention was made to modify the teachings of Hershey with those of Ilgun, by

using a simulator to generate the "designated component bit pattern", because

doing so would enable the user to "model intrusions at a higher level of

transactions than audit records." (See Ilgun: p.183, Section D).

22. In regards to Claim 6, Hershey teaches the following limitations:

6. (Currently Amended) The method of claim 5, wherein:

the respective mathematical function has as arguments:

the value of the quantity calculated at a preceding time step by at least another one of the state machines;
(See Hershey: col.9, line 65 to col.10, line 7, which teaches that "The first FSM is called the predecessor FSM, and it is configured to detect the first component pattern. The second FSM is called the successor FSM, and it is configured to detect the second component pattern. The first FSM will send a starting signal to the second FSM, when the first FSM has successfully detected the first component pattern.")

a respective history of values assumed by the quantity calculated by the respective state machine; and
(See Hershey: col.10, lines 60-65, which teach that "Each memory has a plurality of data storage locations, each having a first portion with n-X bits, to be output to the address register as part of the next address. Many of the memory locations have a second portion which stores a command to reset the address register if the FSM fails to detect its designated component bit pattern.")

a respective control code determined by content present in a memory of the respective device at the time step; and

(See Hershey: col.10, lines 60-65, which teach that "Each memory has a plurality of data storage locations, each having a first portion with n-X bits, to be output to the address register as part of the next address. Many of the memory locations have a second portion which stores a command to reset the address register if the FSM fails to detect its designated component bit pattern.")

However, Hershey does not expressly teach the following limitation:

the respective mathematical function is such that the quantity assumes a stochastic behavior.

Sekar, on the other hand, does teach this. Sekar teaches (Section 4 "Runtime Model", paragraph 2; also Fig.3) that "An EFSA [extended finite-state automata] is normally non-deterministic. ... A deterministic EFSA (DEFA for short) is an EFSA in which at most one of the transitions is enabled in any state of the EFSA."

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Hershey with those of Sekar, because Sekar teaches about the inherent properties of finite-state automata.

Response to Arguments

23. Examiner has applied new art in response to Applicant's amendments to the existing claims and addition of new claims. The arguments pertaining to the previously applied art are therefore no longer relevant.

Allowable Subject Matter

24. The following is a statement of reasons for the indication of allowable subject

matter:

25. In regards to Claim 10, Hershey teaches the following limitations:

10. (New) A method of determining the integrity of a distributed information processing system
including a plurality of networked devices, each device including a finite state machine (FSM), the
method comprising:

   performing a primary task in each of the plurality of networked devices, the primary task
having a computation requirement that varies over time;

Examiner interprets the "primary system with multiple devices" as being a
network of FSMs. Hershey teaches the use of a plurality of security agents and a
network security manager. (See Hershey: col.7, lines 22-50; col.6, lines 46-65;
Fig.24; col.11, line 35 to col.12, line 25)

   performing a secondary task in each of the plurality of networked devices, wherein
performing the secondary task in a first one of the plurality of networked devices includes
generating, per time step, a respective numerical value that depends on a corresponding
numerical value in each of the others of the plurality of networked devices at a previous time step;

(See Hershey: col.9, line 65 to col.10, line 7, which teaches that "The first FSM is
called the predecessor FSM, and it is configured to detect the first component
pattern. The second FSM is called the successor FSM, and it is configured to
detect the second component pattern. The first FSM will send a starting signal to
the second FSM, when the first FSM has successfully detected the first
component pattern." Examiner interprets the "detection" as being a Boolean
mathematical function that determines a numerical value - equivalent to "if x=y
then ..., else ...")

   receiving, at a control server, update information regarding the state of each of the
plurality of networked devices;

Hershey teaches that security agents produce and transmit a security alert
message to a network security manager. (See Hershey: col.7, lines 22-29).

   However, neither Hershey alone, nor in combination with either Ilgun or

Sekar, teach the following combination of limitations, in particular, the step of

determining whether there is a mismatch between the received numerical values

and the simulated numerical values:

   simulating, in the control server, the secondary task of each of the plurality of networked
devices, wherein simulating the secondary task in the control server includes generating, per time
step, numerical values for each of the simulated secondary tasks, based at least upon the
received update information;

        receiving, at the control server, the numerical values generated by the plurality of networked devices; and

        determining whether there is a mismatch between the received numerical values and the simulated numerical values;

        wherein generating the numerical value, per time step, in each of the networked devices, further depends on a history of previous numerical values of the device performing the secondary task, the history has a length, and the length is dynamically modified in inverse relation to the computational requirements of the primary task.

26. Claim 10 and its dependent claims would be allowable if the 35 USC 101 and 35 USC 112, second paragraph rejections were to be overcome.

27. For example, Claims 11 and 12, if both were to be incorporated into Claim 10, would help to provide a utility for Claim 10.

Conclusion

28. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

    A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will

the statutory period for reply expire later than SIX MONTHS from the date of this

final action.

Correspondence Information

Any inquiry concerning this communication or earlier communications from

the examiner should be directed to Ayal I. Sharon whose telephone number is

(703) 306-0297. The examiner can normally be reached on Monday through

Thursday, and the first Friday of a biweek, 8:30 am – 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the

examiner's supervisor, Kevin Teska can be reached on (703) 305-9704. Any

response to this office action should be mailed to:

Director of Patents and Trademarks
Washington, DC 20231

Hand-delivered responses should be brought to the following office:

4th floor receptionist's office
Crystal Park 2
2121 Crystal Drive
Arlington, VA

The fax phone number is: (703) 872-9306

Any inquiry of a general nature or relating to the status of this application

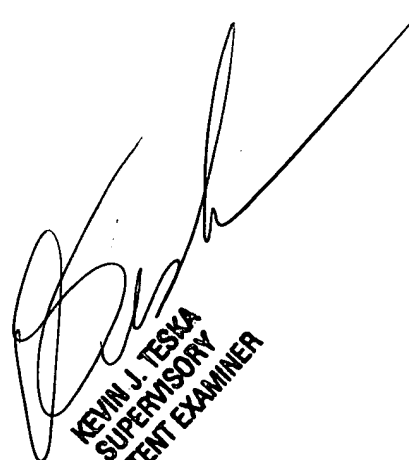or proceeding should be directed to the receptionist, whose telephone number is:

(703) 305-3900.

Ayal I. Sharon

Art Unit 2123

April 16, 2004

KEVIN J. TESKA
SUPERVISORY
PATENT EXAMINER